

CLAIMS:

1. A token issuance and binding process comprising:  
providing a plurality of tokens, each token having a unique ID number  
stored therein;  
generating a unique public/private key pair for each token;  
storing each token ID number and corresponding public key in a  
directory/database;  
storing each private key in its respective token; and  
binding a unique ID number of a user to a corresponding one of the plurality of tokens  
by storing said correspondence there between in the directory/database.
2. The process of claim 1, the binding comprising a Tokenizing Officer  
reviewing credentials of a user and forwarding the user ID number and token ID number  
to a CMS (Certificate Management System) along with E-form request and signature of  
the Tokenizing Officer.
3. The process of claim 2, the binding further comprising the CMS checking  
for redundant user tokens and revoking any such user tokens.
4. The process of claim 3, the binding further comprising the CMS filling in  
the E-form from its directory/database and forwarding the filled in E-form to the  
Tokenizing Officer.

5. The process of claim 4, the binding further comprising the Tokenizing Officer reviewing data in filled in E-form and comparing against user credentials and returning same to CMS after signing.

6. The process of claim 5, the binding further comprising the CMS validating the Tokenizing Officer's signature and generating and wrapping at least a signature certificate/private and associated private key for the user in the unique public key of the token and returning same to the Tokenizing Officer.

7. The process of claim 6, the binding further comprising the Tokenizing Officer storing the signature certificate/private key for the user in the token.

8. The process of claim 7, the binding further comprising the user unwrapping the signature certificate/private key using the token private key stored in the token.

9. The process of claim 1, wherein providing a plurality of tokens comprises providing a plurality of USB (Universal Serial Bus) tokens.

10. The process of claim 1, wherein providing a plurality of tokens comprises providing a plurality of smart cards.

11. A PKI (Public Key Infrastructure) system comprising:

a plurality of tokens, each token having a unique ID number stored therein;

a CMS (Certificate Management System) facility including a first interface to read data from said plurality of tokens and to write data to said plurality of tokens and including a directory/database; and

a badging facility including a terminal operatively connected to communicate with said CMS and including a second interface to read data from said plurality of tokens and to write data to said plurality of tokens;

wherein said CMS generates a unique public/private key pair for each token and stores each token ID number and corresponding token public key in said directory/database and stores each token private key in its respective token; and

wherein a Tokenizing Officer utilizes said terminal in said badging facility to forward a unique ID number of a user to which a particular token is to be issued along with the unique ID number of said particular token to said CMS and wherein said CMS binds the unique ID number of said user to said particular token ID number by storing the correspondence there between in said directory/database.

12. The system of claim 11, wherein said Tokenizing Officer reviews credentials of said user and forwards the user ID number and token ID number to said

CMS along with an E-form request and signature of said Tokenizing Officer.

13. The system of claim 12, wherein said CMS checks for redundant user tokens and revokes any such user tokens.

14. The system of claim 13, wherein said CMS fills in the E-form from said directory/database and forwards the filled in E-form to said Tokenizing Officer.

15. The system of claim 14, wherein said Tokenizing Officer reviews data in filled in E-form and compares against user credentials and returns same to said CMS after signing.

16. The system of claim 15, wherein said CMS validates said Tokenizing Officer's signature and generates and wraps at least a signature certificate and associated private key for said user in said unique token public key of said particular token and returns same to said Tokenizing Officer.

17. The system of claim 16, wherein said Tokenizing Officer stores the signature certificate/private key for said user in said particular token.

18. The system of claim 17, wherein said user unwraps said signature certificate/private key using said token private key stored in said particular token.

19. The system of claim 11, wherein said plurality of tokens comprises a plurality of USB (Universal Serial Bus) tokens.

20. The system of claim 11, wherein said plurality of tokens comprises a plurality of smart cards.